Constructing 2-dimensional Galois representations associated to modular forms of weight 2

CJ Dowd

December 9, 2024

The references for these two talks are Takeshi Saito's IHES notes and Diamond-Shurman Chapter 9.

1 First lecture: Preliminaries and construction (12/2/24)

1.1 Motivation

A fundamental idea in the Langlands program is to give something resembling a bijection between Galois representations and automorphic representations. The simplest case of this is essentially class field theory. Today we will focus on the next simplest case:

Definition 1.1. Let $f = \sum_n a_n q^n \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized Hecke eigen-cusp form. Let $\mathbb{Q}(f)$ denote the field generated by the Hecke eigenvalues of f (equivalently, the field generated by the Fourier coefficients a_n), which is always a number field, and let $\mathbb{Q}(f) \to E_\lambda$ be an embedding of $\mathbb{Q}(f)$ into a finite extension of $\mathbb{Q}_\ell$. We say that a 2-dimensional ℓ-adic Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ is *associated* to f if, for all $p \nmid N\ell$, V is unramified at p and $\mathrm{tr}(\mathrm{Frob}_p) = a_p$.

Theorem 1.2. *Let $N \geq 4$ be an integer and let ε be a Dirichlet character mod N. Let $f \in S_2(N, \epsilon)$ be a normalized eigenform, and let $\lambda \mid \ell$ be a place of $\mathbb{Q}(f)$. Then there exists an ℓ-adic representation $V_{f,\lambda}$ over $\mathbb{Q}(f)_\lambda$ associated to f.*

Some other facts:

- $V_{f,\lambda}$ is unique up to isomorphism and irreducible
- We actually have the stronger condition $\det(1 - \rho(\mathrm{Frob}_p)t) = 1 - a_p t + \epsilon(p)p^{k-1}t^2$.

We will skip over most basic facts related to modular forms, elliptic curves, and Galois representations and get right into the geometric construction.

This talk follows Saito's lecture notes from the 2006 IHES summer school.

1.2 Hecke algebra preliminaries

Let $Y_1(N)$ be the modular curve of level $\Gamma_1(N)$. Recall that (for $N \geq 4$) this represents the functor sending a scheme S to pairs (E, P) consisting of an elliptic curve over S and a point $P \in E(S)[N]$ of exact order N. Its compactification is $X_1(N)$.

The group $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ with the quotient given by the surjective homomorphism $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ sending a matrix to its lower-right entry d mod N. Consequently, $(\mathbb{Z}/N\mathbb{Z})^\times$ acts on $X_1(N)$ by lifting to Mobius transformations, and the action corresponding to $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ is denoted by $\langle d \rangle$ and referred to as a "diamond operator." This is actually the Hecke operator corresponding to the double coset $\Gamma_1(N)\gamma\Gamma_1(N)$ for any $\gamma \in \Gamma_0(N)$ with lower-right entry d mod N, which is actually just the single coset $\Gamma_1(N)\gamma$ due to normality of $\Gamma_1(N)$ in $\Gamma_0(N)$. On points, we have $\langle d \rangle (E, P) = (E, dP)$, noting that dP is a point of exact order N on E if P is, since d is coprime to N.

Let $S_k(\Gamma_1(N))$ denote the space of cusp forms of weight k and level $\Gamma_1(N)$. The group of diamond operators acts on this finite-dimensional space, and since this group is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$, we conclude that $S_k(\Gamma_1(N))$ decomposes as a direct sum of common eigenspaces for the diamond operators, indexed by Dirichlet characters mod N. Given a Dirichlet character ϵ, we let $S_k(N, \epsilon)$ denote the corresponding eigenspace.

The direct sum decomposition $S_k(\Gamma_1(N)) = \bigoplus_\epsilon S_k(N, \epsilon)$ is preserved by the action of the other Hecke operators T_ℓ, since we can show that these commute with the diamond operators on the space of modular forms, so we may further decompose into Hecke eigenforms.

Additionally, we have the *Atkin-Lehner involution*, often denoted w_N or just w, which sends (E, P) to $(E/\langle P \rangle, Q')$, where $Q' \in (E/\langle P \rangle)[N]$ is the unique point that lifts to the point Q in $E[N]$ such that $e_N(P, Q) = \zeta_N$ under the Weil pairing.

The Hecke algebra is $T_k(\Gamma_1(N)) = \mathbb{Q}[T_n, \langle d \rangle] \subseteq \mathrm{End}(S_k(\Gamma_1(N)))$. We can usefully interpret the Hecke algebra as dual to the space of cusp forms:

Proposition 1.3. *The map $S_k(\Gamma_1(N))_\mathbb{C} \to \mathrm{Hom}_{\mathbb{Q}-v.s.}(T_k(\Gamma_1(N), \mathbb{C})$ sending a cusp form to the maps $T \mapsto a_1(Tf)$ is an isomorphism of $\mathbb{C}$-vector spaces. Therefore, $T_k(\Gamma_1(N)$ is a finite $\mathbb{Q}$-vector space, since $S_k(\Gamma_1(N))_\mathbb{C}$ is finite-dimensional.*

In fact, this is an isomorphism of Hecke modules, since the Hecke action of T on $T_k(\Gamma_1(N), \mathbb{C})$ is just defined by pre-composing with multiplication by T, so that $\langle T' \cdot T, f \rangle = a_1(TT'f) = \langle T, T'f \rangle$.

Proof. It suffices to show that the corresponding pairing $\langle T, f \rangle \mapsto a_1(Tf)$ is nondegenerate. If we have a cusp form f such that $a_1(T_\ell f) = 0$ for all ℓ, then by explicit formulas for the Hecke operators we conclude that the q-expansion of f is 0, hence $f = 0$. If T is a Hecke operator such that $a_1(Tf) = 0$ for all f, then the form Tf is in the kernel since $a_1(T'Tf) = a_1(TT'f)$, so by what we already showed we must have $Tf = 0$ for all f, i.e. T is the zero operator. ∎

Corollary 1.4. *The above isomorphism restricts to a bijection between the two finite sets:*

- *Normalized eigenforms $f \in S_k(\Gamma_1(N))_\mathbb{C}$*

- $\mathbb{Q}$-*algebra homomorphisms* $T_k(\Gamma_1(N)) \to \mathbb{C}$ *(not just linear functionals)*

Proof. If f is a normalized cusp eigenform, then the corresponding linear functional sends a Hecke operator T to its eigenvalue λ_T for f, which defines an algebra homomorphism $T_k(\Gamma_1(N)) \to \mathbb{C}$ since eigenvalues of compositions multiply.

Conversely, suppose the linear functional $\varphi : T_k(\Gamma_1(N) \to \mathbb{C}$ corresponding to a cusp form f is an algebra homomorphism. Then we must have $1 = \varphi(1) = a_1(f)$, so f is normalized. We must also have $a_\ell(Tf) = a_1(T_\ell Tf) = \varphi(T)a_\ell(f)$ for every prime ℓ and $T \in T_k(\Gamma_1(N))$, which is enough to imply that f is a Hecke eigenform with T acting by eigenvalue $\varphi(T)$.

Finiteness of $T_k(\Gamma_1(N))$ as an vector space over $\mathbb{Q}$ implies that these sets are finite. This also shows that $\mathbb{Q}(f) \subset \mathbb{C}$ is a number field, since $\mathbb{Q}(f)$ is the image of the homomorphism $\varphi_f : T_k(\Gamma_1(N)) \to \mathbb{C}$. ■

1.3 Wrong way maps on (co)homology, and Hecke correspondences

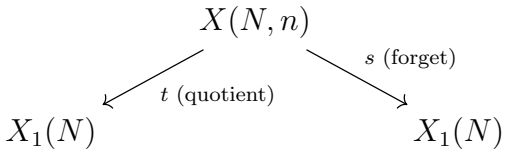
Given $f : X \to Y$, there is a natural pushforward map $H_1(X, \mathbb{Z}) \to H_1(Y, \mathbb{Z})$–just take the image of a cycle under f. Likewise, cohomology naturally pulls back. However, in some cases we can also define "wrong way" maps on (co)homology, going in the opposite of the natural direction. In particular, we can do this for a branched covering map of Riemann surfaces, or a finite flat map of curves.

For homology, if $f : X \to Y$ is a degree d covering map, then given a cycle $\Delta \subset Y$, we can consider the d preimages $f^{-1}(p)$ of a given basepoint $p \in \Delta$ and lift the path Δ to a union of d paths based at these d points. One checks that this construction sends cycles to cycles and boundaries to boundaries. This defines a map $f^* : H_1(Y, \mathbb{Z}) \to H_1(X, \mathbb{Z})$ Likewise, one defines a pushforward $f_* : H^1(X, \mathbb{Z}) \to H^1(Y, \mathbb{Z})$ by dualizing. These maps are usually referred to as "trace" or "transfer" maps. The same idea works for pushing forward sheaf cohomology: the trace is essentially given by a fiber-wise sum.

The transfer maps satisfy a compatibility with cap product: $f^*([\Delta] \cap [\sigma]) = f^*[\Delta] \cap f^*[\sigma]$. One can use this compatibility to extend the definition to a more general setting via Poincare duality, especially since we can show $f^*[Y] = [X]$: we can define $f^*([Y] \cap [\sigma]) = [X] \cap f^*[\sigma]$.

The Hecke operators act on homology and cohomology via finite flat correspondences between modular curves. More specifically, the diamond operators have an obvious action on (co)homology, since $\langle d \rangle$ is an automorphism of $X_1(N)$. However, the Hecke operators T_n don't come from genuine automorphisms on $X_1(N)$. Instead, their action on cohomology is induced by a correspondence as follows.

Suppose $(n, N) = 1$, and let $X(N, n)$ denote the modular curve of level $\Gamma_1(N) \cap \Gamma_0(n)$. It represents the functor sending a scheme $S/\mathbb{Z}[1/nN]$ to triples (E, P, C) consisting of an elliptic curve over S, a point P of exact order N, and a finite flat subgroup $C \subset E$ of order n. There are two natural maps $X(N, n) \to X_1(N)$: we can send the point (E, P, C) to $(E/C, \overline{P})$ (quotienting by the subgroup C) or we can send this point to (E, P) (forgetting the subgroup C):



We can then define the action of the Hecke operator T_n on cohomology by $s_* \circ t^*$, and on homology by $t^* \circ s_*$ (do the "right way" map first, then the transfer map). We abusively denote these actions by T_n^* and $T_{n,*}$, respectively. In our case, we will be considering the action of T_n on the cohomology group $H^0(X_1(N), \Omega^1) = S_2(\Gamma_1(N))$ and on the homology group $H^1(X_1(N), \mathbb{Z})$ and its base changes. Under this definition, we have the compatibility

$$\int_{T_*\gamma} \omega = \int_\gamma T^*\omega.$$

for loops $\gamma \in H_1(X_1(N), \mathbb{Z})$ and forms $\omega \in H^0(X_1(N), \Omega^1)$ and for all Hecke operators T. Consequently:

Proposition 1.5. *There is a canonical isomorphism*

$$H_1(X_1(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathrm{Hom}(S_2(\Gamma_1(N)), \mathbb{C})$$

of $T_2(\Gamma_1(N))_{\mathbb{R}}$-modules.

Proof. Cusp forms of weight 2 may be identified with global sections of $\Omega^1_{X_1(N)}$ on the modular curve. Under this identification, the pairing in the proposition is simply given by integration of a differential form along a loop: $(\gamma, \omega) = \int_\gamma \omega$. ■

1.4 Jacobians of modular curves

Let $\pi : X \to S$ be a smooth proper curve of genus g (i.e. with geometrically connected fibers of genus g), which for simplicity we assume admits a section $s : S \to X$. Define the functor

$$\mathrm{Pic}^0_{X/S}(T) = \frac{\ker(\deg : \mathrm{Pic}(X \times_S T) \to \mathbb{Z}(T))}{\mathrm{Im}(f^* : \mathrm{Pic}(T) \to \mathrm{Pic}(X \times_S T))}$$

Some facts:

- The functor $\mathrm{Pic}^0_{X/S}$ is representable by an abelian scheme $J = \mathrm{Jac}_{X/S}$ over S of relative dimension g.
- If $f : X \to Y$ is a finite flat morphism of proper smooth curves, then there are induced maps $f^* : \mathrm{Jac}_{Y/S} \to \mathrm{Jac}_{X/S}$ (given by pullback of line bundles) and a pushforward map $f_* : \mathrm{Jac}_{X/S} \to \mathrm{Jac}_{Y/S}$, which is harder to define.
- The ℓ-adic Tate module of a g-dimensional abelian variety in characteristic not ℓ is a free $\mathbb{Z}_\ell$-module of rank $2g$. It bears a Galois action.

- We may identify $\mathrm{Jac}_{X/\mathbb{C}}[N] \simeq H_1(X,\mathbb{Z}) \otimes \mathbb{Z}/N\mathbb{Z}$, and consequently $V_\ell \mathrm{Jac}_{X/\mathbb{C}} \simeq H_1(X,\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. These identifications are compatible with the pullback and push-forwards mentioned above. In particular, the Hecke action $T_{n,*}$ on $H_1(X,\mathbb{Q})$ induces a Hecke action on the Tate module. Moreover, the Weil pairing may be canonically identified with the cap product on $H_1(X,\mathbb{Q}) \times H_1(X,\mathbb{Q})$.
- $X_1(N)$ has a model over $\mathbb{Z}[1/N]$. Consequently, we can define the Jacobian over $\mathbb{Z}[1/N]$. This Jacobian is smooth over $\mathbb{Z}[1/N]$, so in particular it has good reduction at all primes not dividing N. Therefore the ℓ-adic representation of $G_\mathbb{Q}$ of degree $2g$ supplied by the Tate module $V_\ell \mathrm{Jac}_{X_\mathbb{Q}/\mathbb{Q}}$ is unramified away from primes dividing ℓN (criterion of Neron-Ogg-Shafarevich).
- On an abelian variety over $\mathbb{F}_p$, the eigenvalues of the Frobenius action on the Tate module all have complex absolute value $\sqrt{q}$ under every complex embedding, i.e. they are Weil p-numbers.

Theorem 1.6. *$V_\ell \mathrm{Jac}_{X_1(N)_\mathbb{Q}}$ is a free $T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}$-module of rank 2.*

Proof. We have identified $\mathrm{Hom}(T_2(\Gamma_1(N))_\mathbb{Q}, \mathbb{Q}) \simeq S_2(\Gamma_1(N),\mathbb{C})$, and we have identified $\mathrm{Hom}(S_2(\Gamma_1(N),\mathbb{C}),\mathbb{C})$ with $H_1(X_1(N),\mathbb{Z}) \otimes_\mathbb{Z} \mathbb{R}$, with both of these isomorphisms respecting the Hecke action. This gives an isomorphism $T_2(\Gamma_1(N))_\mathbb{C} \simeq H_1(X_1(N),\mathbb{R})$ of Hecke modules, which we can descend to an isomorphism $T_2(\Gamma_1(N))_\mathbb{Q}^{\oplus 2} \simeq H_1(X_1(N),\mathbb{Q})$ (with the factor of 2 coming from descending from $\mathbb{C}$ to $\mathbb{Q}$ vs. descending from $\mathbb{R}$ to $\mathbb{Q}$). Hence we also get a Hecke isomorphism $T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}^{\oplus 2} \simeq H_1(X_1(N),\mathbb{Q}) \otimes_\mathbb{Q} \mathbb{Q}_\ell \simeq V_\ell \mathrm{Jac}_{X_1(N)_\mathbb{Q}}$. ∎

Now, let f be a normalized cusp-eigenform, which corresponds to a homomorphism $T_2(\Gamma_1(N))_\mathbb{Q} \to \mathbb{Q}(f)$, hence a homomorphism $T_2(\Gamma_1(N))_{\mathbb{Q}_\ell} \to \mathbb{Q}(f)_\lambda$ for any place $\lambda \mid \ell$ of $\mathbb{Q}(f)$. Hence, we can define the tensor product

$$V_{f,\lambda} := V_\ell(J_1(N)) \otimes_{T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}} \mathbb{Q}(f)_\lambda$$

is 2-dimensional over $\mathbb{Q}(f)_\lambda$. This is a 2-dimensional Galois representation of $G_\mathbb{Q}$ over $\mathbb{Q}(f)_\ell$ (with the Galois group acting only on the Tate module part of the tensor product). This is the Galois representation we are looking for, and it remains to show that this is the Galois representation associated to f. It suffices to work over $J_1(N)_{\mathbb{F}_p}$ instead, since the reduction map induces an isomorphism of ℓ-adic Tate modules and induces the restriction to the decomposition group $D_p = G_{\mathbb{Q}_p}$. As is typical with these types of arguments, the action of the Frobenius morphism matches the action of the Galois-theoretic Frobenius on the Tate module, so we will be able to abuse this identification to extract information about the trace of Frobenius.

To summarize, we've constructed a 2-dimensional Galois representation by considering the Tate module of the modular curve, which carries a Galois action and a Hecke action, and we used the Hecke action and the "system of Hecke eigenvalues" associated to f to squish this into a 2-dimensional representation over $\mathbb{Q}(f)_\lambda$. This representation is unramified at $p \nmid N\ell$. It only remains to show that the trace of Frobenius is correct, which we will do next time.

2 Second day: Eichler-Shimura relation (12/9/24)

Recall that we have constructed a 2-dimensional Galois representation, unramified away from ℓN, defined by

$$\rho = V_{f,\lambda} := V_\ell J_{X_1(N)_{\mathbb{Q}}} \otimes_{T_2(X_1(N))_\ell} \mathbb{Q}(f)_\lambda$$

where f is a weight 2 normalized eigenform and the tensor product is defined by the Hecke action on the left and the homomorphism $T_2(X_1(N)) \to \mathbb{Q}(f)$ sending a Hecke operator to its eigenvalue for f. The main result we want is:

Theorem 2.1. *Let $p \nmid \ell N$. On $V_\ell J_{X_1(N)}$, the action of Frob_p satisfies the polynomial $x^2 - T_p x + \langle p \rangle p = 0$.*

This suffices to prove what we want, since in V_ℓ this means that Frobenius satisfies the polynomial $x^2 - a_p x + \epsilon(p)p = 0$, noting that a_p and $\epsilon(p)$ are the images of T_p and $\langle p \rangle$ in $\mathbb{Q}(f)$, respectively.

To prove this, we use:

Theorem 2.2. (Eichler-Shimura relation.) *For $p \nmid N$, the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)_{\mathbb{Z}[1/N]}) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(X_1(N)_{\mathbb{F}_p}) & \xrightarrow{\sigma_{p,*} + \tilde{\langle p \rangle}_* \sigma_p^*} & \mathrm{Pic}^0(X_1(N)_{\mathbb{F}_p}) \end{array}$$

where the vertical maps are the reduction maps and where σ_p denotes the Frobenius morphism.

Let's review the maps involved here. From the perspective of viewing a Jacobian as $H^0(\Omega^1)^\vee / H_1(\mathbb{Z})$, a Hecke operator T acts on $J(X_1(N))$ by sending an element $\varphi \in S_2(\Gamma_1(N))^\vee \simeq H^0(X, \Omega^1)^\vee$ to $[\varphi \circ T]$. More algebraically, T_p it can be describe as a composition of pullback and pushforwards of the Jacobian:

$$T_p = (\pi_1 \circ \alpha)_* \circ \pi_2^*$$

induced by the correspondence we wrote down before. Recall how we defined "pullback" of singular homology under a finite map: take all of the preimages of a given cycle and add them up. The diamond operator, being a genuine automorphism on $X_1(N)$, acts simply by pushforward. All of this can be phrased algebraically: pushforward of divisors is just taking the image, and pullback can either be interpreted as pullback of line bundles or as taking preimages of divisors with multiplicity. We can describe the action of T_p more easily using the moduli space interpretation of the modular curve. Let $[E, Q]$ denote the divisor class associated to a point on $X_1(N)_{\overline{\mathbb{Q}}}$. Then the T_p action on the Jacobian is given by

$$T_p[E, Q] = \sum_C [E/C, Q \bmod C]$$

where the sum ranges over all order p subgroups of E, of which there are $p+1$ (recall we assume $p \nmid N$, otherwise we need to require that $Q \notin C$). We may similarly describe the action of the diamond operators as

$$\langle d \rangle [E, Q] = [E, dQ].$$

The pushforward and pullback maps on Jacobians induced by a finite morphism of curves $C \to C'$ are compatible with reduction modulo p provided that C and C' have good reduction modulo p. Hence we can safely deduce that $\langle d \rangle_*$ reduces to $\langle d \rangle_*$ modulo p. *However*, we defined the action of T_p on $J(X_1(N))$ via a correspondence, involving the modular curve $X(\Gamma_1(N) \cap \Gamma_0(p))$. This curve does *not* have good reduction modulo p, so we really cannot make sense of the induced action of T_p on the mod p Jacobian using the previous description. Instead, we need to describe the reduction of T_p in terms of Frobenius, which is exactly what the Eichler-Shimura relation does.

If E has ordinary[1] reduction, then one of its order p subgroups stands out: the kernel of the reduction map $E[p] \to E_{\mathbb{F}_p}[p]$, which we denote C_0 and call the *canonical subgroup*.

Lemma 2.3. *Let (E, P) be an elliptic curve with level N structure over $\mathbb{Q}_p$ with ordinary reduction over p. Denoting the reductions with a tilde, we have isomorphisms*

$$(\widetilde{E}/C_0, \tilde{Q} \bmod \tilde{C}_0) \simeq (\tilde{E}^{\mathrm{Frob}_p}, \tilde{Q}^{\mathrm{Frob}_p})$$

or

$$(\tilde{E}^{\mathrm{Frob}_p^{-1}}, p\tilde{Q}^{\mathrm{Frob}_p^{-1}})$$

if $C \neq C_0$.

Proof. We start with the $C = C_0$ case. Let $\phi : E \to E/C =: E'$. Since C_0 descends to local subgroup μ_p on $\tilde{E}$, $\ker \tilde{\varphi}$ is local, so we conclude that $\tilde{E} \to \tilde{E}'$ is totally inseparable. Hence, it factors through the Frobenius map $\tilde{E} \to \tilde{E}^{(\mathrm{Frob}_p)}$, so for degree reasons we obtain an isomorphism $\tilde{E}^{(\mathrm{Frob}_p)} \to \tilde{E}'$, and we can identify the image of $\tilde{Q}$ with $\tilde{Q}^{\mathrm{Frob}_p}$ in $\tilde{E}^{(\mathrm{Frob}_p)}$.

In the case that $C \neq C_0$, we can instead conclude that $\tilde{\varphi} : \tilde{E} \to \tilde{E}'$ is separable, so its dual isogeny $\tilde{\psi} : \tilde{E}' \to \tilde{E}$ is totally inseparable of degree p, hence factors through Frobenius. Thus, as before, we have a factorization of ψ through Frobenius

$$\tilde{E}' \to \tilde{E}'^{\mathrm{Frob}_p} \simeq \tilde{E}$$

Letting $\tilde{Q}' \in \tilde{E}'$ be the image of $\tilde{Q} \in E$, since we must have $\psi(\tilde{Q}') = p\tilde{Q}$, we conclude that $\tilde{Q}'^{\mathrm{Frob}_p}$ is identified with $p\tilde{Q}$ in the above isomorphism. Hence, we conclude that $\tilde{E}' \simeq \tilde{E}^{\mathrm{Frob}_p^{-1}}$ with $\tilde{Q}'$ being identified with $p\tilde{Q}^{\mathrm{Frob}_p^{-1}}$. ∎

[1] One can also sometimes define the canonical subgroup for curves with supersingular reduction if the curve is "not too supersingular" in the sense of the theory of overconvergent modular forms.

This is very close to showing what we want in the Eichler-Shimura relation: it tells us that the reduction of the Hecke action is

$$\widetilde{T_p[E,Q]} = \sum_C [\widetilde{E/C}, \tilde{Q} \bmod C] = [\tilde{E}^{\mathrm{Frob}_p}, \tilde{Q}^{\mathrm{Frob}_p}] + p\langle p\rangle_*[\tilde{E}^{\mathrm{Frob}_p^{-1}}, \tilde{Q}^{\mathrm{Frob}_p^{-1}}].$$

We would like to restate this in terms of pushforward and pullback of the Frobenius morphism σ instead of the Galois action Frob_p. Clearly $[\tilde{E}^{\mathrm{Frob}_p}, \tilde{Q}^{\mathrm{Frob}_p}] = \sigma_*[\tilde{E}, \tilde{Q}]$. We claim that $p[\tilde{E}^{\mathrm{Frob}_p^{-1}}, \tilde{Q}^{\mathrm{Frob}_p^{-1}}] = \sigma^*[\tilde{E}, \tilde{Q}]$. To see this, note that there is exactly one curve $\tilde{E}^{(p)^{-1}}$ for which the relative Frobenius map $\tilde{E}^{(p)^{-1}} \to \tilde{E}$. (This is because p-th roots in characteristic p are unique.) Hence, the point $(\tilde{E}, \tilde{Q})$ on the modular curve mod p has one point in its preimage under Frobenius, which is the point $(\tilde{E}^{\mathrm{Frob}_p^{-1}}, \tilde{Q}^{\mathrm{Frob}_p^{-1}})$ with multiplicity p, as desired. This proves the Eichler-Shimura relation for ordinary points, and one can extend the lemma to supersingular points as well (where the two formulas in the lemma actually coincide, so that we get the same result for all order p subgroups). The rest is then a matter of making sure that everything actually works when we compactify from the moduli space of elliptic curves with level structure to $X_1(N)$, which we are ignoring in this talk (but is mostly just a matter of identifying birational maps).

To finish the proof of Theorem 2.1, we again identify the action of Frob_p on points with σ_* and the action of $p\,\mathrm{Frob}_p^{-1}$ with σ^*. Hence, after tensoring with $\mathbb{Q}(f)_\lambda$, the Eichler-Shimura relation tells us that we have

$$\mathrm{Frob}_p + p\epsilon(p)\,\mathrm{Frob}^{-1} = a_p$$

whence the Frobenius action satisfies the polynomial $x^2 + a_p x + \epsilon(p)p$.

To be more careful really show that this is the characteristic polynomial of Frobenius, we write

$$(1 - \mathrm{Frob}_p\, t)(1 - \epsilon(p)p\,\mathrm{Frob}_p^{-1}\, t) = 1 - a_P t + \epsilon(p)pt^2$$

and taking the determinant of both sides gives

$$\det(1 - \mathrm{Frob}_p\, t)\det(1 - \epsilon(p)p\,\mathrm{Frob}_p^{-1}\, t) = (1 - a_P t + \epsilon(p)pt^2)^2$$

where the determinant on the right hand side follows since all of the coefficients are just scalar. One finally concludes that we have the correct characteristic polynomial of Frobenius by showing that $\det(1 - \mathrm{Frob}_p\, t) = \det(1 - \epsilon(p)p\,\mathrm{Frob}_p^{-1}\, t)$, which involves an argument with the Atkin-Lehner operator w_N.

2.1 Weight ≥ 2 case

To construct Galois representations associated to modular forms of weight > 2, we turn to étale cohomology. Let $f : E_{Y_1(N)} \to Y_1(N)$ be the universal elliptic curve and let $j : Y_1(N) \to X_1(N)$ be the open immersion.

Theorem 2.4. *(*Fancy version of the Eichler-Shimura isomorphism, I think?*) For any $k \geq 2$, we have a canonical isomorphism*

$$H^1_{\text{et}}(X_1(N)_{\mathbb{C}}, j_*(\text{Sym}^{k-2} R^1 f_* \mathbb{Q})) \otimes_{\mathbb{Q}} \mathbb{R} \to S_k(\Gamma_1(N))_{\mathbb{C}}$$

of $T_k(\Gamma_1(N))_{\mathbb{R}}$-modules. This descends to realize

$$H^1_{\text{et}}(X_1(N)_{\mathbb{C}}, j_*(\text{Sym}^{k-2} R^1 f_* \mathbb{Q}_\ell))$$

as a rank 2 free $T_k(\Gamma_1(N))_{\mathbb{Q}_\ell}$-module.

Then, as before, we can define

$$V_{f,\lambda} := H^1(X_1(N)_{\mathbb{C}}, j_*(\text{Sym}^{k-2} R^1 f_* \mathbb{Q}_\ell)) \otimes_{T_k(\Gamma_1(N))_{\mathbb{Q}_\ell}} \mathbb{Q}(f)_\lambda$$

for any weight k eigenform f. It turns out that this is the dual of what we want, i.e. in the representation above, Frob_p^{-1} (the so-called geometric Frobenius) satisfies

$$x^2 + a_p x + \epsilon(p) p^{k-1} = 0$$

. Proving this is thematically the same as the weight 2 case, where we prove an Eichler-Shimura relation that descends the action of T_p on etale cohomology to its action mod p by examining quotients by order p subgroups of an elliptic curve with level N structure.